

CLAIMS

We claim:

1 1. A method of enciphering information constituted by a finite sequence
2 $\{S_1, S_2, \dots, S_N\}$ of N symbols $\{S_1, S_2, \dots, S_N\}$ selected from an alphabet A , wherein there are
3 defined both a secret convention (K) of p key symbols K_1, \dots, K_p selected from a second
4 alphabet B , and a multivariate function M having $m+1$ variables ($m \leq N$): $M(X_{i_1}, \dots, X_{i_m}, Y)$
5 operating $A^m \times B$ in A , $\{i_1, \dots, i_m\}$ being m distinct indices in the range $[1, N]$ and the function
6 M being objective relative to at least one (X_{i_1}) of the m variables of A , said enciphering
7 method comprising:

8 initially placing the N symbols (S_1, S_2, \dots, S_N) constituting the information to be
9 enciphered in the N positions of a shift register, and then

10 performing a succession of X turns of the shift register implementing a
11 succession of X permutations on the sequences $\{S_1, S_2, \dots, S_N\}$ such that where
12 $\{S_1, S_2, \dots, S_N\}$ is the sequence prior to the j^{th} permutation, the sequence after the j^{th}
13 permutation is $\{S_2, S_3, \dots, S_N, Z_j\}$, where Z_j is equal to $M(S_{i_1}, \dots, S_{i_m}, K_j)$, the enciphered
14 information being constituted by the sequence $\{S'_1, S'_2, \dots, S'_N\}$ contained in the shift
15 register at the end of the X^{th} permutation resulting from the X^{th} turn of the shift register.

1 2. An enciphering method according to claim 1, wherein the function
2 $M(X_{i_1}, \dots, X_{i_m}, Y)$ is objective relative to the first variable (X_{i_1}) .

1 3. An enciphering method according to claim 1, wherein the number m is equal to
2 N .

1 4. An enciphering method according to claim 1, wherein the number m is less
2 than N .

1 5. An enciphering method according to claim 1, wherein the number X of
2 permutations is greater than several times the length N of the sequences $\{S_1, S_2, \dots, S_N\}$.

1 6. An enciphering method according to claim 5, wherein the number m is equal to
2 3, the function M being defined by $M(X_1, X_2, X_N, Y)$.

7. An enciphering method according to claim 6, wherein the function $M(X_1, X_2, X_N, Y)$ is calculated using the following steps:

$$U = t1(X_1, X_N)$$

$$V = t2(U, Y)$$

$$Z = t1(V, X_2)$$

$t1$ and $t2$ being the functions associated with two Latin squares $T1$ and $T2$ of size equal to the number N .

8. A method of deciphering information enciphered using the enciphering method of claim 7, wherein the symbols $(S'_1, S'_2, \dots, S'_N)$ of the sequence $\{S'_1, S'_2, \dots, S'_N\}$ constituting the enciphered information are reverse symbol by symbol $(S'_N, S'_{N-1}, \dots, S'_1)$, $M(S_1, S_2, S_N, K_j) = Z_j$ is calculated using a key symbol K_j beginning with the last key symbol to be used during enciphering, and so on in decreasing order $\dots Z_j, Z_{j-1}, \dots$, with $M(X_1, X_2, X_N, Y) = Z$ being calculated using the following steps:

$$V = t1^{\square}(X_1, X_N)$$

$$U = t2^{\square}(V, Y)$$

$$Z = t1^{\square}(U, X_2)$$

the sequence obtained at the end of the X^{th} permutation reconstituting the information in the clear $\{S_1, S_2, \dots, S_N\}$.